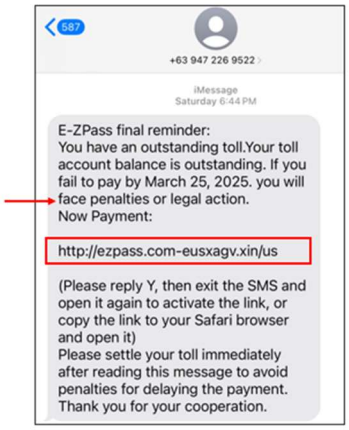
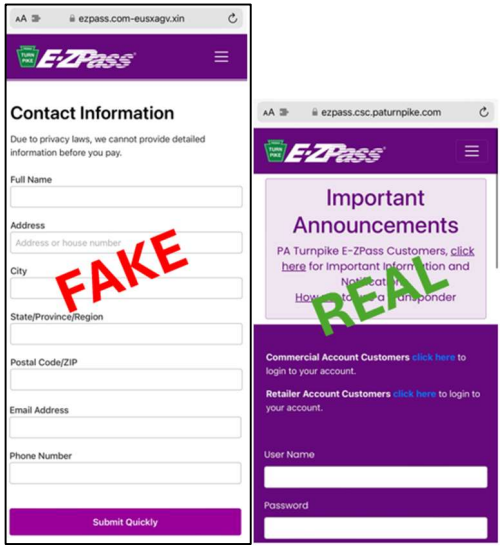
Smishing Toll Scams: How fake texts can turn into a counterfeit mobile wallet

1) Scam: text received from fraudster posing as a toll company; example features an EZPass spoof:

- Penalties & legal action threatened… urgent action required
- + 63 is a Philippines phone number *(EX)*
- .xin is a Chinese-based URL domain *(EX)*

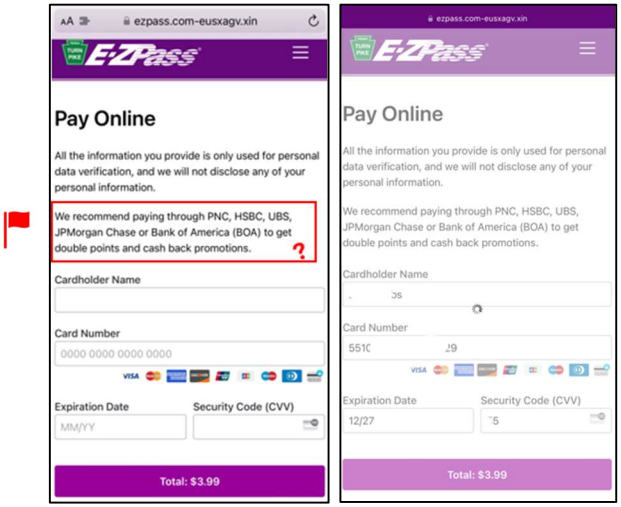


2) Members are taken to a site that closely resembles E-ZPass *(same color scheme as legitimate site, same logo, etc.)* and are prompted to enter sensitive information:

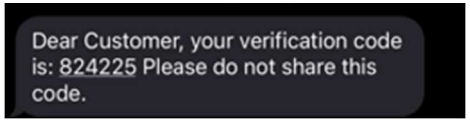


3) Victim is then taken to the "Pay Online" page and prompted to enter their name, card number, expiration date, and 3-digit security code:

- Once the consumer clicks the purple button at the bottom to "pay" $3.99, the screen begins to load
- The card data entered onto the screen is stolen in plain text by the fraudster from the website
- Now, the fraudster will add the victim's card to their mobile wallet

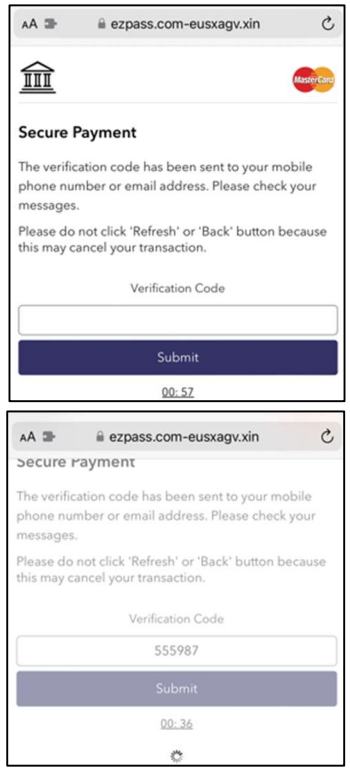


4) Once loading is complete—*i.e, the fraudster is available to verify the card and monitor the information entered into the site*—a "Secure Payment" page instructs the victim to enter a "verification code" sent via email or SMS:



The text sent to the victim is the 6-digit code needed to activate a card on mobile wallet

5) After the code is entered, the screen again defaults to a "loading" state:



6) No transaction occurs. The victim does not think anything of it since nothing was debited from the account, until fraud is seen on the membership when the fraudulent mobile device is used to make tokenized purchases.

For more information about current scams and how to keep your personal information safe, visit service1fcu.com/security-center.

Service 1 FEDERAL CREDIT UNION